

IN THE SPECIFICATION

Please amend the specification as shown below.

Please replace the paragraph beginning on page 1, line 5 with the following:

The present invention generally relates to the processing of binary words by calculation functions. The present invention more specifically relates to the execution, by a state machine in wired logic of an integrated circuit, of a calculation representing a function ~~likely to be~~ capable of being used by several applications within this same circuit.

Please replace the paragraph beginning on page 1, line 11 with the following:

An example of application of the present invention relates to the implementation, within a the same circuit, of several processings all using a same operating function. For example, it may be a public key signature processing, a data integrity control or a random generator for cryptography. In all the above cases, a so-called "Hash" discriminating function is generally used, for example, functions known as SHA, MD5, etc.

Please replace the paragraph beginning on page 2, line 3 with the following:

It could also have been devised to ~~memorize~~ store an intermediary state of an interruptible application to leave the work register and the operator available for another priority-holding application. However, a ~~memorization~~ storing operation followed by a restoring of the states of the work register associated with the operator adversely affects the system performances and weakens it as concerns security against possible piracies of the handled quantities.

Please replace the paragraph beginning on page 3, line 15 with the following:

For clarity, only those steps and those elements which are necessary to the understanding of the present invention have been shown in the drawings and will be described hereafter. In particular, the exploitation made of the calculations by the discrimination function have not been ~~detailed and are no object of the present invention~~ described in detail. Furthermore, the present invention ~~applying~~ applies whatever the application requiring use of the wired operator. Further, the other components of an integrated circuit containing the calculation circuit of the present invention are conventional and have not been described.

Please replace the paragraph beginning on page 3, line 29 with the following:

Circuit 1 ~~essentially~~ comprises a logic operator 2 ($f(\text{PSi-1}, \text{Bi})$) executing an operation using as operands a binary block B and a state PS representing the result of the operation at a previous iteration.

Please replace the paragraph beginning on page 5, line 14 with the following:

Of course, to implement the present invention, the data words to be processed by the discriminating function are also stored in adapted ~~memorization~~ storage elements (for example, registers). Rank i stored in register 3 assigned to the application is used to select the appropriate data block upon resumption of the iterations for the concerned application.

Please replace the paragraph beginning on page 6, line 9 with the following:

Of course, the present invention is likely to have various alterations, modifications, and improvements which will readily occur to those skilled in the art. In particular, the practical forming of the calculation circuit according to the present invention is within the abilities of those skilled in the art based on the functional indications given hereabove. Further, the

Attorney's
Docket No.: S01022.81024

Express Mail Label No.: EV 292 548 153 US

- 4 -

commands necessary to the multiplexer and to the different register by using conventional control means are within the abilities of those skilled in the art. Moreover, although this has not been ~~detailed~~ described in detail, the selection of the block Bi assigned to the data word of the application may be performed in several manners. For example, the integrated circuit CPU manages the reading of the desired blocks according to the decided priorities.